UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/403,071	01/13/2000	TAKUYA NISHIMURA	MTS-V03176	6807

7590 05/06/2004

RATNER & PRESTIA
ONE WESTLAKES BERWYN
PO BOX 980 SUITE 301
VALLEY FORGE, PA 194820980

EXAMINER	
TRAN, TONGOC	

ART UNIT	PAPER NUMBER
2134	11

DATE MAILED: 05/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/403,071	Applicant(s) NISHIMURA ET AL.	
	Examiner Tongoc Tran	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 February 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-9,12,17,22,23 and 31-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☒ Claim(s) *1-3,5-9,12,17,22,23,31-42* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicants' amendment filed on 2/9/2004. Claims 1-3, 6-9, 17, 20, 22-23, 31-33 are amended. Claims 4, 10-11, 13-16,18-19, 21, 24-30 and 43 are canceled. Claims 1-3, 5-9, 12, 17, 20, 22-23 and 31-42 are pending.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 2/9/2004 has been considered by the examiner.

Response to Arguments

3. Applicant's arguments with respect to claims 1-3, 7-9, 17, 20, 22-23 and 31-33 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 17, 20, 22, 23 and 31-33 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Okuyama (U.S. Patent No. 5,987,126) in view of Ekushingu

(JP Patent No. 08-214090) and Al-Tuwaijry et al. (IEE Conference Pubication, "High Speed RSA Processor", 1991, hereinafater Al-Tuwaijry).

In respect to claim 1-3, 17, 20, 22, 23 and 31-33, Okuyama discloses a digital AV data transmitting unit, a receiving unit and a transceiving system and a medium storing program comprising:

data significance deciding means for deciding the significance degree of digital AV data (see col. 9, lines 37-61, a detector);

transmitting-side authentication selecting means for selecting one type of rule from the transmitting-side plurality of authentication rules storing means in accordance with a decision result by the data significance deciding means when receiving an authentication request (see col. 9, lines 37-65); and

transmitting-side authenticating means for performing authentication request (see col. 9, lines 37-65); and

transmitting-side authenticating means for performing authentication in accordance with the selected authentication rule (see col. 9, lines 37-61);

a receiving unit for communicating with a transmitting unit (see Fig. 16);

a receiving unit comprising at least:

an authentication requesting means for requesting the authentication (see col. 9, line 61-col. 10, line 18, channel number request notifier);

receiving-side authentication selecting means for selecting the same authentication rule as the predetermined authentication rule selected by the transmitting-side authentication selecting means (see col. 36, lines 10-22);

received-side authenticating means for performing authentication at the receiving side in accordance with the select authentication rule (see col. 36, lines 10-22); Okuyama discloses an encryptor and a decryptor encrypting and decrypting data corresponding to the channel numbers with copy prohibition specification or copy permit specification for only once by the generation management information but does not explicitly discloses said information is stored in a plurality-of-authentication-rule storing means (see col. 9, lines 37-61, an encryptor). However, Ekushingu discloses a storage mean for plurality of encipher program and decoding programs corresponding to different information access levels (page 3-4, [0021] and [0022] access level (ID number) can be arbitrarily set. For example, it can be set for each music...category of music...popularity stakes of the music...whether the music is a new song...). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize a storing mean to store plurality of encryption for the purpose of providing encryption for different level of access needs.

Furthermore, Okuyama does not disclose wherein the plurality of types of authentication rules includes a first rule configured to use a public key and a secret key to provide a first type of encryption having high-security against forgery or alteration, and a second rule configured to use a common key to provide a second type of encryption having low-security against forgery or alteration.

However, Al-Tuwaijry discloses the private key system (e.g. DES) are more widely used than the public key systems because they are fast and easy to implement, but provide low security and the public key system (e.g. RSA) provide much higher

security levels but they are very slow (see Abstract). Therefore, it would have been obvious to one of ordinary skill in the art a the time the invention was made to incorporate the teaching of Okuyama's encryption and decryption system according to different channels with Ekushingu's teaching of storage means of plurality of encryption schemes according to different access levels and Al-Tuwaijry's teaching of public key being more secure than common key for the benefit of achieving desirable speed according to security level of data (see Al-Tuwaijry, Abstract, paragraph 2).

In respect to claims 5, 6 and 12, Okuyama further discloses the transmitting unit has the functions of the receiving unit and the receiving unit has the function of the transmitting unit (see col. 9, lines 61-65);

wherein three or more of the receiving units having the functions of the transmitting unit are connected each other so that digital AV data can be transferred to each other (see Fig. 23, and col. 27, lines 40-50).

5. Claims 34-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Okuyama (U.S. Patent No. 5,987,126) in view of Ekushingu (JP Patent No. 08-214090, English Translation) and Al-Tuwaijry (IEE Conference Pubication, "High Speed RSA Processor", 1991) and further in view of Jones (U.S. Patent No. 5,655,077).

In respect to claims 34-42, Okuyama further disclose wherein the control criterion is capable of identifying an illegal or legal digital AV data receiving unit; and cancels the authentication when the ID is unqualified for authentication (see col. 19, lines 45-56) but does not explicitly discloses said control criterion is a reference list. However, Jones

discloses a list is provided for authenticating authorized computer (see col. 9, lines 20-24). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide a predetermined reference list to identify an authorized receiver for faster and convenient data transmission.
Furthermore, Okuyama discloses an information identification to identified the device (see col. 8, lines 38-43) but does not discloses using signature generated from an ID of the receiving unit to authenticate receiving unit. However, Jones discloses using digital signature technique to verify authorized system in a logon procedure. It would have been obvious to one of ordinary skill in the art at the time the invention was made to provide the use of digital signature for the benefit of its secure verification technique.

6. Claims 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicants' own admitted prior art in view of Ekushingu (JP Patent No. 08-214099) and Okuyama (U.S. Patent No. 5,987,126) and Al-Tuwaijry (IEE Conference Pubication, "High Speed RSA Processor", 1991).

In respect to claims 7-9, Applicants' admitted prior art discloses a digital AV data transmitting unit, a receiving unit and a transceiving system comprising:

unit authentication rule information receiving means for receiving the information for one type of authentication rule owned by a digital AV data receiving unit;
transmitting-side authentication rule fetching means for fetching an authentication rule owned by the digital AV data receiving unit in accordance with the information for the authentication rule received by the unit authentication rule information receiving means;

and transmitting-side authenticating means for performing the authentication in accordance with the fetched authentication rule (see Applicants' admitted prior art drawing, Fig. 2, specification pages 1-3, background art).

Applicants' admitted prior art teaches a storing means for storing a single type of authentication rules but does not teach a storing means for a plurality of types of authentication rules. However, Ekushingu discloses an encryption and decryption program storage means to memorize the encryption and decryption program corresponding to different information access level. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize a storing mean to store plurality encryption needs for the purpose of providing encryption according to different level of access needs.

Applicants' admitted prior art does not disclose but Okuyama discloses data significance deciding means for deciding the significance degree of digital AV data; transmitting-side authentication selecting means for selecting one type of authentication rule from the transmitting-side plurality of authentication-rule in accordance with a decision result by the data significance deciding means (see col. 9, lines 37-65). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the data deciding means and authentication selecting means in order to provide different level of encryptions according to different level of copy protection.

Applicants' admitted prior art does not disclose wherein the plurality of types of authentication rules includes a first rule configured to use a public key and a secret key

to provide a first type of encryption having high-security against forgery or alteration, and a second rule configured to use a common key to provide a second type of encryption having low-security against forgery or alteration.

However, Al-Tuwaijry discloses the private key system (e.g. DES) are more widely used than the public key systems because they are fast and easy to implement, but provide low security and the public key system (e.g. RSA) provide much higher security levels but they are very slow (see Abstract). Therefore, it would have been obvious to one of ordinary skill in the art a the time the invention was made to incorporate the teaching of Okuyama's encryption and decryption system according to different channels with Ekushingu's teaching of storage means of plurality of encryption schemes according to different access levels and Al-Tuwaijry's teaching of public key being more secure than common key for the benefit of achieving desirable speed according to security level of data (see Al-Tuwaijry, Abstract, paragraph 2).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

-Tatebayashi et al. Disclose information devices which select and use one out of plurality of encryption utilization protocols for protecting copyrights of digital productions.

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Examiner Tongoc Tran
Art Unit: 2134

TT

April 21, 2004

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137